Subject: Data Classification Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>January 1, 2012</td>
<td>1 of 6</td>
</tr>
</tbody>
</table>

Purpose:
The purpose of this policy is to identify the different types of data, to provide guidelines and examples for each type of data, and to establish the default classification for data.

Scope:
This policy applies to all data produced, collected, stored or used by Fordham University, its employees, student workers, consultants or agents during the course of University business.

Data Classification Types
All data covered by the Scope of this policy will be classified as Fordham Protected data, Fordham Sensitive data, or Fordham Public data.

Fordham Protected data
Fordham Protected data is any data that contains personally identifiable information concerning any individual, as well as any data that contains personally identifiable information that is regulated by local, state, or Federal privacy regulations, and any data designated or described by any voluntary industry standards or best practices concerning protection of personally identifiable information that Fordham chooses to follow. These regulations may include, but are not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standards (PCI DSS)

Examples of some of the types of data that are regulated are listed in the appendix.

Fordham Sensitive data
Fordham Sensitive data is any data that is not classified as Fordham Protected data, but which is classified by the department originating or maintaining custody of the data as being proprietary information. Custodians or Owners of data classified as Fordham Sensitive data identify data as Fordham Sensitive data based on their internal standard operating procedures. Examples of the type of data included are: budgets, salary and raise information, and possible properties that Fordham may be interested in purchasing.

This is a “Related Policy” as defined in section B of the “IT Policy Statement” section of the “Fordham IT Acceptable Use Policy”, which is at www.fordham.edu/itpolicy. In the event that IT Security and IT Risk Management protocols or procedures are published, any deviation may only be done in concert with the University Information Security Office with sufficient time to allow for appropriate risk analysis, documentation and possible presentation to authorized University representatives. Willful failure to adhere to published policy or protocol may be met with University sanctions.
Subject: Data Classification Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>January 1, 2012</td>
<td>2 of 6</td>
</tr>
</tbody>
</table>

Fordham Public data
Fordham Public data is any data that Fordham intends to make available to the general public. For department-specific data, this classification comes from the department. If data is created jointly by more than one department, all involved departments and custodians will meet and will jointly classify the data. If they are unable to agree on the classification, the data is classified as Fordham Sensitive Data, and remains designated as Fordham Sensitive data until the custodians of the data reach an agreement to reclassify the data or until an administrator with the authority establishes the classification. For University-wide data, classification is assigned only by the Office of the President, the Office of Registrar, Academic Affairs, or Institutional Research. Examples of the types of data include, but are not limited to: department faculty lists, department addresses, press releases, and the Fordham web site. Data that does not contain personally identifiable information concerning any individual, and that is not Fordham Protected data or Fordham Sensitive data, is classified as Fordham Public data.

Default classification of data
Any data that contains personally identifiable information concerning any individual or that is covered by local, state, or Federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that Fordham chooses to follow, is classified as Fordham Protected data by default. All other data is classified as Fordham Sensitive data by default.

Questions about this policy
If you have questions about this policy, please contact the Information Security Office at infosec@fordham.edu

This is a “Related Policy” as defined in section B of the “IT Policy Statement” section of the “Fordham IT Acceptable Use Policy”, which is at www.fordham.edu/itpolicy. In the event that IT Security and IT Risk Management protocols or procedures are published, any deviation may only be done in concert with the University Information Security Office with sufficient time to allow for appropriate risk analysis, documentation and possible presentation to authorized University representatives. Willful failure to adhere to published policy or protocol may be met with University sanctions.
Appendix: Fordham Protected Data

Listed below are examples of types of personally identifiable information protected by local, state, or Federal privacy regulations. These examples do not constitute an exhaustive list of all types of information that are protected by local, state, or Federal privacy regulations. If owners or custodians are in doubt about the status of data in their custody, they should contact the Office of IT Risk and Data Integrity at extension 3108.

Examples:

- Social security numbers
- Credit card and debit card numbers
- Bank account numbers and routing information
- Driver’s license numbers and state identification card numbers
- Student education records
  - **Bursar's Office**: Student account files and Perkins loan information
  - **Departments and Colleges**: Academic advising records, admission files, including but not limited to ACT, SAT and TOEFL scores, and other evaluative data as well as high school and college transcripts and other scholastic records.
  - **Directory Information**:
    - Name
    - Address(es) and telephone number
    - University e-mail address
    - Photograph
    - Major and minor field(s) of study, including the college, division, department, institute or program in which the student is enrolled
    - Dates of attendance
    - Grade level (such as freshman, sophomore, junior, senior or graduate level)
    - Enrollment status (undergraduate or graduate, full-time or part-time)
    - Date of graduation
    - Degree(s) received
    - Honors or awards received, including selection to a dean's list or honorary organization
    - Participation in officially recognized activities or sports
    - University e-mail address
    - Weight and height of members of athletic teams
Subject: Data Classification Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>January 1, 2012</td>
<td>4</td>
</tr>
</tbody>
</table>

- Financial Aid: Financial assistance application files, student federal work-study information, scholarships and Stafford loan information pertaining to students, applicants or their representatives
- Intercollegiate Athletics: Injury reports, incident reports, scholarship contacts, performance records, height and weight information
- Registration and Records: Permanent record of academic performance (grades, transcript, including supporting documents), course schedules
- Residence Life: Residential life and housing services files
- Student Life: Student activity files, student disciplinary files, multi-cultural programs and services files, and intramural sports files
- Student Services: Career planning files, including placement information and employers' files, international programs and services files
- Undergraduate Admission and other admission offices: Admission files on prospective students
- University Library: Circulation records, records of use of any material controlled by the library including but not limited to purchase requests.

- Personal health records
  - Patient information: addresses, dates, telephone/fax numbers, social security numbers, medical records numbers, patient account numbers, insurance plan numbers, vehicle information, license numbers, medical equipment numbers, photographs, fingerprints or other biometric information, e-mail and Internet addresses. **Note:** Personal health records stored in education records are subject to FEPRA and are excluded from HIPAA.

This is a “Related Policy” as defined in section B of the “IT Policy Statement” section of the “Fordham IT Acceptable Use Policy”, which is at www.fordham.edu/itpolicy. In the event that IT Security and IT Risk Management protocols or procedures are published, any deviation may only be done in concert with the University Information Security Office with sufficient time to allow for appropriate risk analysis, documentation and possible presentation to authorized University representatives. Willful failure to adhere to published policy or protocol may be met with University sanctions.
Additional Information about referenced regulations

FERPA
FERPA is a Federal law that protects the privacy of student education records. This law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA provides students with the right to inspect and review certain education records maintained by the school and to request corrections if the records are inaccurate or misleading. It requires that schools obtain written permission before releasing information from a student’s education record. It also allows schools to publish certain “directory” information about students, unless the student has requested that the school not do so.
The penalty for failing to comply with FERPA is loss of all federal funding, including grants and financial aid.

Additional information is available at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

GLBA
GLBA protects consumers’ personal financial information held by financial institutions. It requires that financial institutions provide customers with a privacy notice explaining what information is collected, how it is used, and how it is protected.
The penalty for failing to comply with GLBA is a fine of up to $100,000 for the institution and of up to $10,000 for the officers and directors of the institution.
Additional information can be found at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

HIPAA
HIPAA protects the privacy of Protected Health Information (PHI). It establishes regulations for the use and disclosure of PHI, including a patient’s health status, provision of health care, medical records or payment history.
Penalties for wrongfully disclosing PHI range from a $50,000 to a $250,000 fine and a one year to a ten year prison term, depending on the circumstances. These fines are for the individual, not the institution.
Additional information can be found at http://www.hhs.gov/ocr/hipaa/.

Payment Card Industry Data Security Standards (PCI DSS)
PCI DSS is an industry standard which protects credit card customer account data. The PCI DSS standard requires organizations that accept credit cards for payment to utilize a secure network and to adhere to specific procedures and standards to protect credit card data. Failing to comply...
with PCI DSS can result in significant fines. Credit card providers can fine merchants up to $500,000 per compromise if it is established that the merchant was not complaint at the time at which data was compromised. Merchants may also be banned from accepting certain types of credit cards.

Additional information is available at https://www.pcisecuritystandards.org/tech/index.htm.

Additional US State Laws
If you work for Fordham inside the United States but outside of New York, please send an email containing the state in which you work to infosec@fordham.edu. The Information Security Office will respond to you by providing you with information about any additional privacy laws that apply to you.